P.B.5818 – Patentlaan 2
2280 HV Rijswijk (ZH)
+31 70 340 2040
TX 31651 epo nl
FAX +31 70 340 3016

Europäisches Patentamt
Zweigstelle in Den Haag
Recherchen-abteilung

European Patent Office
Branch at The Hague
Search division

Office européen des brevets
Département à La Haye
Division de la recherche

ABB Patent Attorneys
c/o ABB Schweiz AG,
Intellectual Property (CH-LC/IP),
Brown Boveri Strasse 6
5400 Baden
SUISSE

Frist

Datum/Date
30.06.04

Zeichen/Ref./Réf.	Anmeldung Nr./Application No./Demande n°./Patent Nr./Patent No./Brevet n°.
03/071 EP	03405896.6-2413-

Anmelder/Applicant/Demandeur/Patentinhaber/Proprietor/Titulaire
ABB RESEARCH LTD.

COMMUNICATION

The European Patent Office herewith transmits as an enclosure the European search report for the above-mentioned European patent application.

If applicable, copies of the documents cited in the European search report are attached.

☒ Additional set(s) of copies of the documents cited in the European search report is (are) enclosed as well.

The following specifications given by the applicant have been approved by the Search Division:

☒ abstract ☐ title

☐ The abstract was modified by the Search Division and the definitive text is attached to this communication.

The following figure will be published together with the abstract: 2

REFUND OF THE SEARCH FEE

If applicable under Article 10 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 40 5896

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 6 405 318 B1 (ROWLAND CRAIG H) 11 June 2002 (2002-06-11) * abstract * * column 2, line 40 - line 67 * * column 4, line 30 - column 6, line 67 * * column 8, line 8 - line 45 * * figures 9,10 *	1-10	G06F1/00 G06F21/00 H04L29/06
A	WO 03/083660 A (STUTE MICHAEL ;GLOBAL DATAGUARD INC (US)) 9 October 2003 (2003-10-09) * the whole document *	1-10	
A	WO 02/23808 A (CYMTEC SYSTEMS INC) 21 March 2002 (2002-03-21) * the whole document *	1-10	
A	US 2002/093527 A1 (SHERLOCK KIERAN G ET AL) 18 July 2002 (2002-07-18) * the whole document *	1-10	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

G06F
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	9 June 2004	Horn, M.P.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 40 5896

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-06-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6405318 B1	11-06-2002	AU 3737400 A	28-09-2000
		WO 0054458 A1	14-09-2000
WO 03083660 A	09-10-2003	WO 03083660 A1	09-10-2003
WO 0223808 A	21-03-2002	AU 9086101 A	26-03-2002
		WO 0223808 A2	21-03-2002
US 2002093527 A1	18-07-2002	AU 6676401 A	02-01-2002
		AU 6695501 A	02-01-2002
		AU 6840801 A	02-01-2002
		AU 6849101 A	02-01-2002
		AU 6849201 A	02-01-2002
		AU 6987001 A	02-01-2002
		AU 7131501 A	02-01-2002
		AU 7542701 A	02-01-2002
		WO 0199031 A2	27-12-2001
		WO 0199349 A2	27-12-2001
		WO 0199343 A2	27-12-2001
		WO 0198932 A2	27-12-2001
		WO 0199002 A2	27-12-2001
		WO 0199371 A2	27-12-2001
		WO 0199372 A2	27-12-2001
		WO 0199373 A2	27-12-2001
		US 2004030796 A1	12-02-2004
		US 2004039942 A1	26-02-2004
		US 2003061506 A1	27-03-2003
		US 2003208689 A1	06-11-2003
		US 2002069200 A1	06-06-2002
		US 2002053033 A1	02-05-2002

This application is covered by the extended European search report pilot project at present running within the European Patent Office, applied to all European patent applications filed as first filing and searched on or after 01.07.03. Under this project the EPO issues together with the search report an opinion on whether the application and the invention to which it relates meet the requirements of the EPC. This non-binding opinion is issued free of charge as a service. This opinion may be used as the basis for an informed decision as to whether it is desired to pursue the application further or not.

For further details of this pilot project, the applicant's attention is directed to the Official Journal edition 5/2003. If any further immediate questions or comments arise the EPO Customer Services: +31-70-340 4500 or +49-89-2399 2828 can be contacted.

The attached opinion reveals that the application or the invention to which it relates appear not to meet the requirements of the Convention (see comments on enclosed Form 2906).

If the applicant wishes to continue with this application the examination fee must be paid. Where appropriate amendments can be filed to address the objections raised in the opinion, thus shortening the overall procedure. If no amendments are filed, the opinion will be re-issued as the first official communication under Article 96(2) and Rule 51(2) EPC.

If the examination fee has already been paid and the right to the communication under Article 96(1) EPC has been waived for this application, the first official communication under Article 96(2) and Rule 51(2) EPC will be issued promptly.

The examination is being carried out on the **following application documents**:

Text for the Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT RO SE SI SK TR LI

Description, pages:

1-13 as originally filed

Claims, No.:

1-10 as originally filed

Drawings, sheets:

1/4-4/4 as received on 26.03.2004 with letter of 24.03.2004

*****

1 The following document (D) is referred to in this communication; the numbering will be adhered to in the rest of the procedure:

D1: US-B1-6405318

2 Claims 1, 2, 3, 8 and 10 are not clear in the sense of Art. 84 EPC.

2.1 Claim 1 is not clear because they fail to specify to which entity the "input module" belongs to or, in other words, for which entities the "input module" serves as an input (for the data sources or for the processing module?). The claim is thus not clear for a man skilled in the art from its wording alone and has to be clarified (EPC Guidelines C-III, 4.1).

2.2 The frequent use of the conjunction pair "and/or" in claims 1, 3 and 8 and the enumerations of features in claims 2 and 3 together with the statement "and any combination thereof" render the subject-matter for which protection is sought unclear due to the amount of possible alternatives introduced by this wording. It is

therefore not possible to examine the entire scope of protection of these claims. The claims have to be clarified (EPC Guidelines C-III, 3.7).

2.3 Claim 3 is not clear because it refers to additional features which are not part of independent apparatus claim 1 per se. Indeed, claim 1 refers to a network security system whereas claim 3 specifies how numerical and textual values are "maintained" (EPC Guidelines C-III, 4.8a). The claim has to be clarified.

2.4 Claim 10 is not clear because it specifies "said status and trend presenting means", "the supervisory system" and to "said countermeasures initiating means" without an antecedent definition of these terms. Instead, there is precedent subject-matter relating to "displaying means" and "reaction facilities". The wording of the claim has to be adapted (EPC Guidelines C-III, 4.1, 4.2).

2.5 Independent claim 10 has to contain all essential technical features and should not refer to the subject-matter of other claims in particular when this subject-matter relates to different entities (EPC Guidelines C-III, 4.8a). The reference to other claims has to be removed or claim 10 has to be reformulated as a dependent claim which appears to be possible in the present case.

2.6 Claim 10 specifies "an automation system operator workstation **in** a network **with** an automation system [...]" which induces ambiguity regarding the subject-matter for which protection is sought. It is not clear if the claim relates to an automation system operator workstation or to an automation system comprising a system operator workstation and a network (see EPO-Guidelines C-III, 4.8b). The claim has to be clarified.

2.7 Furthermore, claim 10 introduces ambiguity regarding the subject-matter for which protection is sought by specifying: "system operator workstation **being connected** to a security system" (EPC Guidelines C-III, 4.8a). Indeed, the claim defines its subject-matter by reference to another entity. The claim has to be clarified by, for example, specifying "**connectable**".

3 As far as independent claim 1 is clear it does not fulfill the requirements of Article 52(1) EPC because its subject-matter is not new in the sense of Article 54(1) and

(2) EPC.

3.1 Document D1 discloses, in terms of claim 1, a network security system for detecting security relevant irregularities in a network (column 2, lines 40-41: "*The present invention provides a real-time* ***intrusion detection*** *method and* ***system***"), comprising

data sources located on and constituting the network, with means for generating network-security relevant data (column 8, lines 12-16: "*Each host 151-153 comprises a* ***local controller that sends information*** *about log auditing, login anomaly detection, logout anomaly detection, session monitoring and port scan detector functions* ***to the central controller.***"; figure 9);

an input module [for a processing module], with input handlers for various protocols to connect to the data sources (follows implicitly from column 8, lines 12-16: "*Each host 151-153 comprises a* ***local controller that sends information*** *about* ***log auditing, login anomaly detection, logout anomaly detection, session monitoring*** *and* ***port scan detector functions to the central controller.***"; figure 9);

at least one processing module, connected to said input module for access to said data sources, with means for translating said network-security relevant data into quantitative variables (column 8, lines 16-20: "*The* ***central controller can perform*** *centralized* ***auditing of events*** *154,* ***data analysis*** *155,* ***cross correlation of intrusion activity*** *throughout the network 156 [...]*"; column 8, lines 38-40: "*The system administrator may also alter the* ***alarm thresholds*** *or use preprogrammed alarm thresholds 168.*", figures 9, 10);

a supervisory system, with means for presenting processed data to a security system operator (column 8, lines 16-20: "*The* ***central controller*** *[...]* ***can alert the network system administrator*** *157 if anomalous activity is found.*"; column 8, lines 40-42: "*The system administrator may select* ***whether a warning is to be displayed on the system administrators graphical user interface*** *169.*" figures 9, 10);

and an interface module, with means for transferring said quantitative variables from the processing module to the supervisory system (follows implicitly from column 8, lines 40-42: "*The system administrator may select whether a warning is to be displayed on the system administrators graphical user interface 169.*"; figure 10).

Since all features of independent claim 1 are known in combination from document D1, the subject-matter of claim 1 is not new (Art. 54(1)(2) EPC). Consequently, claim 1 is not allowable (Art. 52(1) EPC).

3.2 It should be noted that even if the applicant were to interpret claim 1 in such a manner as to enable him to allege that its subject-matter was novel, based on minor differences between the features of these claims and those disclosed in document D1, the subject-matter of claim 1 would still not involve an inventive step according to Articles 52(1) and 56 EPC. This due to the fact that, having regard to document D1, the same object and the same type of solution as defined in claim 1 is disclosed.

3.3 Insofar as claim 10 can be understood, it does not involve an inventive step according to Article 56 EPC. The integration of the supervisory system and the countermeasure initiating means of a network security system into the respective means of an automation system operator workstation is a juxtaposition (see also EPO Guidelines, Annex to Chapter IV, 2.1) of known devices functioning in their normal way and not producing any non-obvious working interrelationship. This view is also in-line with the problem statement on page 6, paragraph 3 of the description: providing the display to a person available round-the-clock which is often the case for a process operator of an automation system. An unexpected technical effect of the integration of these two different system cannot be recognized.

4 Dependent claims 2-9 do not contain any additional features that would lead to patentable subject-matter as they are either disclosed in document D1 (claims 2, 3, 4, 5, 9) or are non-technical as they refer to the mere representation of information (claims 6, 7, 8).

5 It is not at present apparent which part of the application could serve as a basis for a new, allowable claim. Should the applicant nevertheless regard some particular matter as patentable, an independent claim should be filed taking account of Rule 29(1) EPC. **The applicant should also indicate in the letter of reply the difference of the subject-matter of the new claim vis-à-vis the state of the art (especially vis-à-vis document D1) and the significance thereof.**

Furthermore, the following points should be dealt with when filing a new set of claims:

5.1 The independent claims should be in the two-part "characterized" form required by rule 29(1) EPC, having a pre-characterising part that correctly reflects the closest prior-art.

5.2 The features of the claims should be provided with reference signs placed in parentheses to increase the intelligibility of the claim (Rule 29(7) EPC). This applies to both the preamble and characterising portion (see EPO-Guidelines, C-III, 4.11)

5.3 To meet the requirements of Rule 27(1)(b) EPC, the document D1 should be identified in the description and the relevant background art disclosed therein should be briefly discussed.

5.4 The introductory portion of the description should be adapted to the new claims. Particularly, following from the disclosure of document D1, **the statement indicating the technical problem to be solved by the invention requires a revision** which should be effected taking the requirements of Rule 27(1)(c) EPC into account (see EPO-Guidelines C-II, 4.5).

6 Care should however be taken during the revision, especially of the introductory portion and any statements of problem or advantage, not to add subject-matter which extends beyond the content of the application as originally filed (Article 123(2) EPC).

In order to facilitate the examination of the conformity of the amended application

with the requirements of Article 123(2) EPC, the applicant is requested to clearly identify the amendments carried out, irrespective of whether they concern amendments by addition, replacement or deletion, and to indicate the passages of the application as filed on which these amendments are based.

If the applicant regards it as appropriate these indications could be submitted in handwritten form on a copy of the relevant parts of the application as filed.